Guard

podręcznik użytkownika

Guard: podręcznik użytkownika

data wydania piątek, 24. lipiec 2015 Version 2.0.0

Spis treści

1 Informacje o tej dokumentacji

Poniższe informacje pozwolą sprawniej posługiwać się tą dokumentacją.

- Jaka jest grupa docelowa niniejszej dokumentacji?
- Jaka jest zawartość niniejszej dokumentacji?
- Dodatkowa pomoc

Jaka jest grupa docelowa niniejszej dokumentacji?

Niniejsza dokumentacja jest skierowana do użytkowników, którzy chcą szyfrować komunikację e-mail i pliki, chroniąc je przed nieuprawnionym dostępem.

Jaka jest zawartość niniejszej dokumentacji?

Niniejsza dokumentacja zawiera następujące informacje:

- W sekcji *Do czego służy aplikacja Guard?* znajduje się opis aplikacji Guard.
- . W sekcji *Korzystanie z aplikacji Guard* znajdują się informacje dotyczące usługi Guard

. Niniejsza dokumentacja przedstawia mechanizmy pracy z typową instalacją i konfiguracją oprogramowania do pracy grupowej. Wersja, której używasz, może różnić się od przedstawionej w tym dokumencie.

Dodatkowa pomoc

Pełna dokumentacja oprogramowania do pracy grupowej znajduje się w podręczniku użytkownika programu OX App Suite.

2 Do czego służy aplikacja Guard?

Guard jest składnikiem zabezpieczeń oprogramowania do pracy grupowej umożliwiającym szyfrowanie wiadomości e-mail i plików.

- Szyfruj korespondencję e-mail prowadzoną z innym użytkownikami lub partnerami zewnętrznymi.
- Zaszyfruj pojedynczy plik i podziel się zaszyfrowanymi danymi z innymi użytkownikami.
- Określaj poziom szyfrowania za pomocą opcji zabezpieczeń.
- Szyfrowane dane są chronione hasłem. Aby uchronić się przed skutkami utraty hasła, korzystaj z funkcji resetowania go.

3 Korzystanie z aplikacji Guard

Dowiedz się, jak pracować z aplikacją *Guard*.

- Stosowanie ustawień podstawowych
- Szyfrowanie korespondencji e-mail
- szyfrowanie plików
- Stosowanie ustawień zabezpieczeń

3.1 Konfiguracja aplikacji *Guard*

Przed użyciem aplikacji *Guard* trzeba skonfigurować kilka ustawień podstawowych.

- Przede wszystkim należy wprowadzić hasło aplikacji Guard Security służące do szyfrowania danych oraz uzyskiwania dostępu do nich.
- Wpisz dodatkowy adres e-mail, który będzie przydatny w sytuacji, gdy zapomnisz hasła aplikacji Guard Security. Pozwoli to na użycie funkcji jego resetowania i wysłanie do Ciebie nowego hasła. Z powodów bezpieczeństwa zdecydowanie zalecamy skonfigurowanie tej funkcji. W przeciwnym razie nowe hasło zostanie wysłane na główne konto e-mail.

Istnieją dwa sposoby wprowadzania ustawień podstawowych:

- Zdefiniuj podstawowe ustawienia podczas pierwszego użycia funkcji szyfrowania.
- Zdefiniuj podstawowe ustawienia na stronie ustawień oprogramowania do pracy grupowej przed pierwszym użyciem funkcji szyfrowania.

Jak zdefiniować podstawowe ustawienia podczas pierwszego użycia funkcji szyfrowania:

1. Włącz funkcję szyfrowania podczas tworzenia wiadomości e-mail, szyfrowania pliku lub przesyłania nowego pliku, klikając ikonę **Szyfrowanie** .
2. Pojawi się monit o wpisanie hasła aplikacji Guard Security oraz dodatkowego adres e-mail. Wpisz odpowiednie dane.

Jak zdefiniować podstawowe ustawienia podczas pierwszego użycia funkcji szyfrowania:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij pozycję **Ustawienia aplikacji Guard Security** na pasku bocznym.

   W przypadku wybrania ustawień aplikacji Guard Security po raz pierwszy pojawi się okno *Utwórz klucze aplikacji Guard Security*.
3. W polu **Hasło** wprowadź hasło, którego chcesz używać do szyfrowania danych.

   Potwierdź hasło, wprowadzając je ponownie w polu **Zweryfikuj**.
4. W polu **Wprowadź nowy zapasowy adres e-mail** wprowadź adres e-mail umożliwiający odebranie hasła tymczasowego podczas resetowania hasła aplikacji Guard Security.
5. Kliknij przycisk **OK**.

3.2 Szyfrowanie rozmów e-mail

Dostępne są następujące możliwości:

- Odczytywanie zaszyfrowanych rozmów e-mail
- Wysyłanie zaszyfrowanych wiadomości e-mail
- Dostęp dla odbiorców zewnętrznych

3.2.1 Odczytywanie zaszyfrowanych rozmów e-mail

Aby przeczytać zaszyfrowaną wiadomość e-mail, trzeba znać co najmniej hasło aplikacji Guard Security. Nadawca zaszyfrowanej wiadomości e-mail może ją zabezpieczyć dodatkowym hasłem.

Jak przeczytać zaszyfrowaną wiadomość e-mail:

1. Wybierz wiadomość e-mail z ikoną *Szyfrowanie* . W widoku szczegółów pojawi się powiadomienie *Zabezpieczona wiadomość e-mail. Wpisz hasło aplikacji Guard Security.*
2. Wprowadź hasło aplikacji Guard Security.

   Można ustawić długość pamiętania hasła. Aby to zrobić, wybierz opcję **Nie wylogowuj mnie z aplikacji Guard**. Wybierz z listy odpowiednią wartość.

   Nadawca mógł zabezpieczyć wiadomość e-mail dodatkowym hasłem. W takim przypadku pojawi się jeszcze jedno pole wejściowe, w którym należy wprowadzić dodatkowe hasło.
3. Kliknij przycisk **OK**. Zawartość pojawi się w formie zwykłego tekstu.

   Jeśli wiadomość e-mail ma załączniki, pojawią się funkcje obsługi załączników w formie zaszyfrowanej lub odszyfrowanej.

Uwaga: w przypadku korzystania z szyfrowanej korespondencji e-mail można tylko odpowiedzieć na tę wiadomość lub przesłać ją dalej.

3.2.2 Wysyłanie zaszyfrowanych wiadomości e-mail

Dostępne są następujące możliwości:

- Wysyłanie zaszyfrowanych wiadomości e-mail. Treść wiadomości e-mail będzie dostępna tylko dla nadawcy i odbiorcy wiadomości.

  Ostrzeżenie: Podczas wysyłania wersji roboczej szyfrowanej wiadomości e-mail, wysłana wersja robocza zostanie usunięta z folderu *Wersje robocze*.
- Wysyłanie wiadomości e-mail z podpisem. Podpis zapewnia możliwość potwierdzenia przez odbiorcę nienaruszenia przesłanej wiadomości e-mail.
- Wysyłanie zaszyfrowanych wiadomości e-mail z podpisem

Jak wysłać zaszyfrowaną wiadomość e-mail:

1. Napisz wiadomość e-mail w aplikacji *E-mail* tak jak to zwykle robisz.

   Na stronie *Nowa wiadomość e-mail* kliknij widoczną w prawym górnym rogu ikonę **Szyfruj**

   Możesz także kliknąć dostępne po lewej stronie polecenie **Opcje zabezpieczeń** i włączyć opcję **Wyślij zaszyfrowane (PGP)**.
2. Aby dodatkowo podpisać wiadomość e-mail, kliknij polecenie **Podpisz e-mail**.

   Jeśli klient e-mail odbiorcy nie obsługuje standardu PGP, lecz wiadomość powinna być czytelna mimo tego, włącz opcję **Użyj PGP w tekście (zgodność)**. Po włączeniu tego ustawienia nie będzie możliwe wysyłanie wiadomości e-mail w formacie HTML.
3. Kliknij pozycję **Wyślij bezpieczną**.

   W przypadku wysyłania wiadomości do odbiorców zewnętrznych pojawi się okno umożliwiające wysłanie im uwag dotyczących otwarcia zaszyfrowanej wiadomości e-mail [12].

3.2.3 Dostęp dla odbiorców zewnętrznych

Zaszyfrowane wiadomości e-mail możesz także wysyłać do odbiorców zewnętrznych nieużywających oprogramowania do pracy grupowej. Po pierwszym wysłaniu zaszyfrowanej wiadomości e-mail do odbiorcy zewnętrznego wykonywane są następujące czynności:

- Tworzone jest automatycznie specjalne konto dla odbiorcy zewnętrznego.
- Możesz określić, czy odbiorca zewnętrzny ma otrzymać automatyczne powiadomienie o zaszyfrowanej wiadomości e-mail, czy niestandardowe.
- Odbiorca zewnętrzny otrzymuje wiadomość e-mail z powiadomieniem i automatycznie utworzonym hasłem.

  Oprogramowanie do pracy grupowej możesz skonfigurować tak, aby odbiorca musiał dodatkowo podać przekazany niezależnie 4-cyfrowy kod PIN do nadanego hasła.
- Odbiorca zewnętrzny otrzymuje wiadomość e-mail z łączem do strony umożliwiającej mu zalogowanie się na specjalnym koncie.
- Odbiorca zewnętrzny wprowadza automatycznie utworzone hasło na stronie logowania.

  Następnie odbiorca musi zmienić automatycznie utworzone hasło. Na wypadek, gdyby je zapomniał i musiał zresetować konto po utracie hasła, konieczne jest wprowadzenie pytania zabezpieczającego oraz odpowiedzi.

  Pojawi się zaszyfrowana wiadomości e-mail.
- Odbiorca zewnętrzny może wysłać zaszyfrowaną odpowiedź na tę wiadomość e-mail.

Po wysłaniu kolejnej wiadomości e-mail do zewnętrznego odbiorcy wykonywane są następujące czynności.

- Odbiorca zewnętrzny otrzymuje wiadomość e-mail z łączem do strony umożliwiającej mu zalogowanie się na specjalnym koncie.
- Na stronie logowania odbiorca wprowadza hasło skonfigurowane po pierwszym otrzymaniu zaszyfrowanej wiadomości e-mail.

  Odbiorca, który nie pamięta hasła, może ustawić nowe. Należy w tym celu odpowiedzieć na pytanie zabezpieczające.

3.3 Szyfrowanie plików

Dostępne są następujące możliwości:

- Szyfrowanie plików
- Tworzenie nowych zaszyfrowanych plików
- Otwieranie zaszyfrowanych plików
- Pobieranie zaszyfrowanych plików
- Odszyfrowywanie plików

3.3.1 Szyfrowanie plików

W przypadku szyfrowania plików zostaną zaszyfrowane tylko ich ostatnie wersje. Wszystkie inne wersje zostaną usunięte.

Jak zaszyfrować plik:

Ostrzeżenie: w przypadku szyfrowania pliku zostaną usunięte wszystkie jego wersje — oprócz bieżącej. Aby zachować starszą wersję, należy ją zapisać przed zaszyfrowaniem pliku.

1. W aplikacji *Pliki* kliknij plik w widoku szczegółów. W wyskakującym okienku kliknij ikonę **Więcej** ☰▾. Kliknij w menu pozycję **Szyfruj**.

   Możesz też wybrać plik. Kliknij dostępną na pasku narzędzi ikonę **Więcej** ☰▾. Kliknij w menu pozycję **Szyfruj**.
2. Jeśli plik zawiera wiele wersji, pojawi się okno *Szyfrowanie plików*. Potwierdź, że chcesz zaszyfrować plik i usunąć wszystkie poprzednie wersje, klikając przycisk **OK**.

   Jeśli plik ma tylko jedną wersję, zostanie on zaszyfrowany bez dalszych monitów.

3.3.2 Tworzenie nowych zaszyfrowanych plików

Nowy zaszyfrowany plik możesz utworzyć, przesyłając plik lokalny z szyfrowaniem.

Jak utworzyć nowy zaszyfrowany plik:

1. Otwórz folder w drzewie folderów.

   Uwaga: Otwórz folder, w którym masz uprawnienia do tworzenia obiektów.
2. Kliknij dostępne na pasku narzędzi polecenie **Nowy**. Kliknij polecenie **Prześlij nowy plik**.
3. W oknie *Prześlij nowe pliki* kliknij polecenie **Wybierz plik**. Wybierz dowolną liczbę plików.

   Kliknij widoczną w prawym górnym rogu ikonę **Szyfruj**🔓.
4. W polu *Opis* możesz wpisać informacje o pliku.
5. Kliknij pozycję **Szyfruj** na pasku menu.

Wskazówka: Nowy zaszyfrowany plik możesz także utworzyć, przeciągając go z pulpitu systemu operacyjnego do okna aplikacji *Pliki* i upuszczając w górnej części okna.

3.3.3 Otwieranie zaszyfrowanych plików

Zaszyfrowany plik możesz otworzyć i przeczytać. Plik będzie nadal zapisany na serwerze w zaszyfrowanej postaci.

Jak otworzyć zaszyfrowany plik:

1. W aplikacji *Pliki*, w widoku szczegółów kliknij wybrany plik. W wyskakującym okienku kliknij polecenie **Zaszyfruj i otwórz**.
2. W oknie *Wprowadź hasło aplikacji Guard Security* wprowadź hasło aplikacji Guard Security.

   Można ustawić długość pamiętania hasła. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość.

   Kliknij przycisk **OK**.

3.3.4 Pobieranie zaszyfrowanych plików

Zaszyfrowany plik możesz pobrać, aby go lokalnie przeczytać lub zmodyfikować. Plik będzie nadal zapisany na serwerze w zaszyfrowanej postaci.

Jak pobrać zaszyfrowany plik:

1. W aplikacji *Pliki* kliknij plik w widoku szczegółów. W wyskakującym okienku kliknij ikonę **Więcej** ☰▾. Kliknij w menu pozycję **Pobierz odszyfrowane**.

   Uwaga: Jeśli w okienku wyskakującym klikniesz polecenie **Pobierz**, pobrany plik pozostanie zaszyfrowany.
2. W oknie *Wprowadź hasło aplikacji Guard Security* wprowadź hasło aplikacji Guard Security.

   Kliknij przycisk **OK**.

3.3.5 Odszyfrowywanie plików

Aby usunąć szyfrowanie z pliku, należy go odszyfrować.

Jak odszyfrować plik:

1. W aplikacji *Pliki* kliknij zaszyfrowany plik w widoku szczegółów. W wyskakującym okienku kliknij ikonę **Więcej** ☰▾. Kliknij w menu pozycję **Usuń szyfrowanie**.

   Możesz też wybrać plik. Kliknij dostępną na pasku narzędzi ikonę **Więcej** ☰▾. Kliknij w menu pozycję **Usuń szyfrowanie**.
2. W oknie *Wprowadź hasło aplikacji Guard Security* wprowadź hasło aplikacji Guard Security.

   Można ustawić długość pamiętania hasła aplikacji Guard Security. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość.

   Kliknij przycisk **OK**.

3.4 Wylogowywanie się z aplikacji Guard

Z aplikacji Guard możesz się wylogować bez zamykania oprogramowania do pracy grupowej. Aby potem otworzyć zaszyfrowane wiadomości e-mail, pliki lub foldery, musisz ponownie wpisać hasło aplikacji Guard Security.
Uwaga: Ta funkcja jest dostępna wyłącznie po włączeniu funkcji **Pamiętaj hasło** przy otwieraniu zaszyfrowanej wiadomości e-mail lub zaszyfrowanego pliku.

Jak się wylogować z aplikacji Guard Security:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu.
2. Wybierz z menu polecenie **Wyloguj z aplikacji Guard**.

3.5 Ustawienia aplikacji Guard

Dostępne są następujące możliwości:

- Aby zmienić ustawienia hasła aplikacji Guard Security, użyj opcji Ustawienia zabezpieczeń aplikacji Guard.
- Aby zmienić domyślne ustawienia wysyłania zabezpieczonych wiadomości e-mail, użyj opcji Ustawienia domyślne aplikacji Guard.
- Możesz także wykonać czynności administracyjne dla kluczy PGP.

3.5.1 Ustawienia zabezpieczeń aplikacji Guard

Dostępne są następujące możliwości:

- zmiana hasła aplikacji Guard Security.
- Jeśli zapomnisz hasła aplikacji Guard Security, możesz je zresetować, żądając wysłania hasła tymczasowego na dodatkowy adres e-mail.
- zmiana dodatkowego adresu e-mail

Jak zmienić hasło aplikacji Guard Security:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij pozycję **Ustawienia aplikacji Guard Security** na pasku bocznym.
3. W polu **Wprowadź bieżące hasło aplikacji Guard Security** w obszarze *Hasło* wprowadź hasło służące dotychczas do szyfrowania danych.

   W polu **Wprowadź nowe hasło aplikacji Guard Security** wprowadź hasło, którego chcesz używać do szyfrowania danych od tej pory.

   Potwierdź hasło, wprowadzając je ponownie w polu **Zweryfikuj nowe hasło aplikacji Guard Security**.
4. Kliknij pozycję **Zmień hasło aplikacji Guard Security**.

Jak zresetować hasło aplikacji Guard Security:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij pozycję **Ustawienia aplikacji Guard Security** na pasku bocznym.
3. Kliknij pozycję **Zresetuj hasło aplikacji Guard Security**. Na Twój zapasowy adres e-mail zostanie wysłane nowe hasło.

   Jeśli nie został wprowadzony dodatkowy adres e-mail, nowe hasło zostanie wysłane na podstawowy adres e-mail.
4. Nowe hasło od razu zostanie bieżącym hasłem aplikacji Guard Security. Należy je natychmiast zmienić.

Jak zmienić dodatkowy adres e-mail do resetowania hasła do szyfru:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij pozycję **Ustawienia aplikacji Guard Security** na pasku bocznym.
3. W polu **Wprowadź bieżące hasło aplikacji Guard Security** w obszarze *Zapasowy adres e-mail* wprowadź hasło służące do szyfrowania danych.

   W polu **Wprowadź nowy zapasowy adres e-mail** wprowadź adres e-mail umożliwiający odebranie hasła tymczasowego podczas resetowania hasła aplikacji Guard Security.

   Kliknij pozycję **Zmień adres e-mail**.

3.5.2 Ustawienia domyślne aplikacji Guard

Ustawienia domyślne określają gotowe ustawienia wprowadzane podczas tworzenia wiadomości e-mail. Możesz je zmienić przed wysłaniem wiadomości.

Jak zmienić ustawienia domyślne:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Na pasku bocznym kliknij pozycję **Ustawienia aplikacji Guard PGP**.
3. Wybierz jedną z opcji pod nagłówkiem *Ustawienia szyfrowania PGP*.

Dostępne są następujące ustawienia.

Wybierz domyślnie wysyłanie szyfrowanych wiadomości e-mail

Wskazuje, czy nowa wiadomość e-mail ma być domyślnie szyfrowana za pomocą PGP.

Domyślnie podpisuj wysyłane wiadomości

Wskazuje, czy nowa wiadomość e-mail ma być domyślnie szyfrowana za pomocą PGP.

Ustaw domyślnie PGP jako PGP w tekście (w celu zachowania zgodności)

Wskazuje, że szyfrowanie PGP ma być realizowane w tekście. Użyj tej opcji, jeśli wiadomość powinna być czytelna mimo tego, że klient e-mail odbiorcy nie obsługuje szyfrowania PGP. Po włączeniu tego ustawienia nie będzie możliwe wysyłanie wiadomości e-mail w formacie HTML.

3.5.3 Zarządzanie kluczami

Do wysyłania i otrzymywania zaszyfrowanych wiadomości funkcje zarządzania kluczami nie są przeważnie potrzebne. Można ich użyć, gdy potrzebna jest realizacja następujących zadań:

- Chcesz użyć kluczy aplikacji Guard PGP w innych klientach e-mail, np. lokalnych.
- Masz klucze PGP z innych aplikacji i chcesz je wprowadzić do aplikacji Guard.
- Chcesz wprowadzić klucz publiczny partnera zewnętrznego do aplikacji Guard, aby odczytywać zaszyfrowane wiadomości od niego.
- Chcesz przekazać klucz publiczny odbiorcy, aby umożliwić mu odczytywanie Twoich zaszyfrowanych wiadomości bez konieczności wchodzenia na serwer kluczy.

Jak otworzyć stronę do zarządzania kluczami:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Na pasku bocznym kliknij pozycję **Ustawienia aplikacji Guard PGP**.

Strona zawiera następujące elementy:

- Opcje pozwalające na dopasowywanie domyślnych ustawień aplikacji Guard
- Sekcja *Twoje klucze* zawierająca funkcje do zarządzania prywatnymi i publicznymi kluczami PGP.
- Sekcja *Klucze publiczne* wyświetlająca klucze publiczne współdzielone przez Ciebie lub innych użytkowników. Jeśli na liście znajduje się klucz publiczny użytkownika, możesz założyć, że może on odszyfrowywać wiadomości e-mail.

Dostępne są następujące funkcje:

- pobranie klucza publicznego
- wysłanie klucza publicznego przez e-mail
- dodawanie nowych kluczy do istniejących przez przesłanie kluczy lokalnych lub utworzenie nowych kluczy w aplikacji Guard
- pobranie klucza prywatnego
- przesłanie klucza publicznego partnera zewnętrznego

Jak pobrać klucz publiczny:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij polecenie **Pobierz klucz publiczny PGP** dostępne poniżej opcji *Twoje klucze*.

Jak wysłać klucz publiczny przez e-mail:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij przycisk **Wyślij e-mailem swój klucz publiczny PGP** widoczny poniżej opcji *Twoje klucze*.

Jak dodać nowe klucze:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Dodaj** + widoczną obok elementu *Lista Twoich kluczy* w sekcji *Twoje klucze*. Pojawi się okno *Dodawanie kluczy*.
3. Dostępne są następujące możliwości:
   - Aby dodać klucz prywatny, kliknij przycisk **Prześlij prywatny klucz**. Wybierz plik z kluczem prywatnym. Pojawi się okno *Przesyłanie kluczy prywatnych*.

     Aby przesłać nowy klucz, wpisz hasło aplikacji Guard Security. Wpisz nowe hasło do nowego klucza.
   - Aby dodać klucz publiczny, kliknij przycisk **Prześlij tylko klucz publiczny**. Wybierz plik z kluczem publicznym.
   - Aby utworzyć nową parę kluczy, kliknij polecenie **Utwórz nowe klucze**. Pojawi się okno *Tworzenie nowych kluczy aplikacji Guard Security*.

     Wpisz hasło do nowego klucza i potwierdź je.

   Nowy klucz zostanie wprowadzony niżej na liście *Lista Twoich kluczy*.

Jak pobrać klucz prywatny:

Uwaga: Pobranie klucza prywatnego na komputer lokalny może stanowić zagrożenie bezpieczeństwa. Pamiętaj, aby zadbać o prywatność klucza prywatnego.

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij umieszczoną obok podpisu ikonę **Pobierz** .

Jak przesłać klucz publiczny partnera zewnętrznego:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Dodaj** widoczną obok + polecenia *Lista kluczy publicznych PGP* poniżej sekcji *Klucze publiczne*. Wybierz plik z kluczem publicznym.

Indeks